

**REMARKS**

This Amendment is submitted in response to the Office Action dated March 1, 2005, having a shortened statutory period set to expire June 1, 2005.

On October 13, 2004, Applicants filed "Amendment A" responsive to a first Office Action dated July 16, 2004, having a shortened statutory period set to expire October 16, 2004. In Applicant's responsive Amendment, Claims 1, 7, 12, 18, 23 and 29-33 were amended. (Applicant's Auto-Reply Facsimile Transmission and Amendment A are attached.)

Applicants are most appreciative of the time and courtesy extended by the Examiner during a teleconference held on May 25, 2005. During that teleconference, it was agreed that the Examiner, due to the USPTO failing to properly enter the October 13, 2004 amendment, did not examine the pending claims as previously amended. For example, the features claimed in exemplary Claim 1 were not examined, which include:

during power up initialization before an operating system is started, copying security data from an unsecure memory device in a computer to a restricted portion of the computer's system memory which is invisible to the operating system, wherein the restricted portion of the computer's system memory contains code and data needed for low level system control functions that are independent of the operating system, and wherein a writing of data into the restricted portion of the computer's system memory is authorized only for a trusted software entity that has been authenticated as having permission to access the restricted portion of the computer's system memory.

Applicants now re-urge the arguments presented in the October 13, 2004 Amendment, and request that either a new non-final Office Action or a Notice of Allowance be issued for the pending claims.

**CONCLUSION**

No extension of time for this response is believed to be necessary. However, in the event an extension of time is required, that extension of time is hereby requested. Please charge any fee associated with an extension of time as well as any other fee necessary to further the prosecution of this application to **IBM CORPORATION DEPOSIT ACCOUNT No. 50-0563.**

Respectfully submitted,



James E. Boice  
Registration No. 44,545  
DILLON & YUDELL LLP  
8911 North Capital of Texas Highway  
Suite 2110  
Austin, Texas 78759  
512.343.6116

ATTORNEY FOR APPLICANT(S)

### REMARKS

This Amendment is submitted in response to the Office Action dated July 16, 2004, having a shortened statutory period set to expire October 16, 2004. In the present Amendment, Claims 1, 7, 12, 18, 23 and 29-33 are amended. Claims 1-33 are now pending.

Applicants are most appreciative of the time and courtesy extended by the Examiner during teleconferences held on September 16 and October 12, 2004. While the teleconferences were very helpful in addressing the issues of the present office action, no agreement was reached regarding informally proposed amendments, which are now formally submitted herein.

### REJECTIONS UNDER 35 U.S.C. § 102

In the present Office Action, Claims 1-33 are rejected under 35 U.S.C. § 102(e) as being anticipated by *Novoa, et al.* (U.S. Patent No. 6,223,284 – "*Novoa*").

*Novoa* teaches a method and system for remotely flashing a system ROM. If access to the system ROM requires an administrator password, that password is either in a "black box" (secure memory device) in the computer (col. 3, lines 10-25), or is part of a remote management package used to flash the system ROM (col. 13, lines 19-44).

### THE CITED PRIOR ART DOES NOT TEACH OR SUGGEST ALL OF THE LIMITATIONS OF THE PRESENTLY CLAIMED INVENTION

With reference to exemplary Claim 1, the cited prior art does not teach or suggest:

during power up initialization before an operating system is started, copying security data from an unsecure memory device in a computer to a restricted portion of the computer's system memory which is invisible to the operating system, wherein the restricted portion of the computer's system memory contains code and data needed for low level system control functions that are independent of the operating system, and wherein a writing of data into the restricted portion of the computer's system memory is authorized only for a trusted software entity that has been authenticated as having permission to access the restricted portion of the computer's system memory.

Specifically, *Novoa* does not teach or suggest copying security data from a nonsecure memory device in a computer. Rather, *Novoa* teaches copying security data from a secure (black box) memory device in the computer or from a packet outside the computer.

Furthermore, *Novoa* does not teach or suggest copying the security data to a restricted portion of the computer's system memory, wherein the restricted portion of the computer's system memory contains code and data needed for low level system control functions that are independent of the operating system, and wherein a writing of data into the restricted portion of the computer's system memory is authorized only for a trusted software entity that has been authenticated as having permission to access the restricted portion of the computer's system memory. Rather, *Novoa* teaches flashing an administrator password to a system ROM, but does not specify any restriction parameters on the system ROM.

For example, with regards to exemplary Claim 31, *Novoa* does not teach or suggest that the restricted portion of the computer's system memory is the SMI memory space.

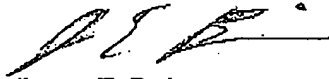
As the cited prior art does not teach or suggest all of the limitations of the present invention as claimed, Applicants respectfully request a notice of allowance for all pending claims.

**CONCLUSION**

Applicants now respectfully request a Notice of Allowance for all pending claims.

No extension of time for this response is believed to be necessary. However, in the event an extension of time is required, that extension of time is hereby requested. Please charge any fee associated with an extension of time as well as any other fee necessary to further the prosecution of this application to **IBM CORPORATION DEPOSIT ACCOUNT No. 50-0563**.

Respectfully submitted,



James E. Boice  
Registration No. 44,545  
DILLON & YUDELL LLP  
8911 North Capital of Texas Highway  
Suite 2110  
Austin, Texas 78759  
512.343.6116

ATTORNEY FOR APPLICANT(S)